EHTEL
EUROPEAN HEALTH TELEMATICS ASSOCIATION

ETHICAL Principles for eHealth: Conclusions from the Consultation of Ethics Experts around the Globe

A Briefing Paper

Funded by
ETHICAL
SEVENTH FRAMEWORK PROGRAMME
Science in Society

A synopsis of outcomes of the ETHICAL project relevant for eHealth

Foreword

Trust and credibility are at heart of any relationship, this counts all the more for healthcare. Preconditions for this are ethical principles and personal values. If eHealth stakeholders are aiming for sustainability, this must be grounded in responsible thus ethically based activities. It is therefore crucial to reflect about ethical determinants and conditions related to eHealth.

With this Briefing Paper, EHTEL aims to reinforce its role as an integrative enabler. Beyond its activities as a platform and networking node, EHTEL is now creating added value for all healthcare stakeholders by producing reports and publications. I would like to thank all those who contributed to writing this publication and highlight the acknowledgements below.

This document has been prepared to provide Members and Friends of EHTEL with an overview of the work of the ETHICAL 7th Framework project. The project was concerned with the ethical issues that surround the collection, use and retention of medical and biometric data. This report concentrates on those aspects of the project that were associated with medical data. Using extracts from the project's deliverables, it highlights ethical issues that have a bearing on the design, delivery and operation of eHealth developments.

The issues contained in this briefing paper affect all stakeholders in eHealth and I recommend that all EHTEL members take time to read through it. The full set of ETHICAL deliverables is available at http://www.ethical-fp7.eu/

EHTEL is determined to support all eHealth and healthcare stakeholders. This is one of a series of publications designed to assist in creating the delivery of high-quality healthcare for all, supported and enhanced by eHealth.

Martin D. Denz, EHTEL President

Acknowledgements

In preparing this paper EHTEL would like to acknowledge the contributions given by:

- The Members of the ETHICAL Consortium (See Annex A)
- David Garwood, Director of the EHTEL Board and main author of this document
- Stephan Schug, EHTEL Chief Medical Officer and EHTEL lead for ETHICAL
- Diane Whitehouse, The Castlegate Consultancy

Contents

Executive Summary

With this Briefing Paper, EHTEL would like to offer all healthcare stakeholders including politicians, citizens, patients, health professionals, healthcare providers, health insurers and many others an insight into some of the key ethical issues identified by ETHICAL, a project co-financed within the 7th Framework Programme.

EHTEL aims to support all stakeholders in the deployment of eHealth by providing an insight into the many ethical issues associated with the deployment of eHealth and to develop an understanding that will reduce the barriers that impinge on progress in this area.

The ETHICAL project was launched in March 2009 with funding from DG Research under the European Commission's 7th Framework Programme.

The project conducted its work over a period of 21 months, completing its activity in December 2011. Work was undertaken by a number of organisations (detailed in Annex A) that conducted academic research and facilitated an international debate conducted using the Delphi method[1] and various interactive fora.

The project considered a range of ethical issues relating to the collection, use and storage of both biomedical and biometric information. This paper concerns itself with those issues that affect eHealth applications. It covers six main areas, namely:

- Trust
- Privacy
- Ownership
- Dignity
- Equity
- Proportionality.

Academic research reveals much interesting information in the field of ethics. In Stage 1 of the Delphi dialogue conducted in ETHICAL, there was a diversity of opinion indicated among the experts as they were able to express their personal views without reference to other opinions. In the later stages of the dialogue, however, an interesting consensus emerged. It was, for example, agreed that:

⇨ Researchers have an ethical responsibility to ensure that the subjects of their research have fully understood the implications of taking part in it.

⇨ Research subjects should always have the right to receive a verbal explanation from a third party unconnected with the research about how their information will be used.

[1] The Delphi method was developed by the RAND Corporation in the 1950s. Using the method, experts are asked to answer questionnaires in two or more rounds with a facilitator providing a summary of the views expressed. These views are subsequently ranked using Likert scales in an iterative process with the experts reviewing their position in the light of others' responses so as to work towards a consensus view.

⇨ Personal medical information is owned by the individual to whom it relates.

Whereas there was a tendency to disagree that:

⇨ The data subject is the only person who can define what is an acceptable level of risk to their personal medical information.

⇨ Personal medical information is co-owned by the patient and the clinician.

This briefing paper identifies a number of key implications for eHealth deployment arising out of the ETHICAL projects work. These can be summarised, at a high level, as:

1 All stakeholders engaged in the development of eHealth initiatives is that they need to integrate resources in project planning to ensure that they have provided sufficient time for transparency in order to meet the ethical requirements of the work.

2 For privacy to be addressed in an ethical manner, eHealth stakeholders will need to address the two areas of consent and security. Properly informed consent requires "disclosure of all necessary information that a reasonable person would use in making an informed decision, in a format that is readily understandable to the individual, and without coercion influencing choice." In support of processes to ensure informed consent is the requirement for all eHealth implementations to have appropriate security measures in place that are commensurate with the sensitivity of the data they hold.

3 However, if it is accepted – and this seems to be the case – that patients have either ownership or control of their medical records, then the question of whether they need to give consent for their data to be stored, shared or traded for any purpose has to be an integral component of the eHealth ecosystem. As to whether such consent can be implied or must be explicit and informed may vary with circumstances.

4 In order to preserve the dignity of the patient policy makers and politicians need to reinforce their claims that "the patient is at the centre of the healthcare process" by establishing an appropriate advocacy process to ensure patients are supported in protecting themselves from inappropriate use of their persons, information and technology.

5 Before eHealth can be shown to be contributing to equality in healthcare, significant planning and action on the part of policy makers and a commitment to widespread investment and deployment will be required.

6 Those responsible for the deployment of eHealth applications that involve the collection, use and storage of personal information will need to consider the issues of proportionality either to avoid offending ethical principles or established legislation

More results and detailed information can be found in Deliverable 2.2, "Dialogue Results" at http://www.ethical-fp7.eu/ .

Part 1 of this paper describes the need for the project, its context and approach while Part 2 describes some of the issues and results of the dialogue in specific areas of ethical interest. Part 3 includes a brief summary and conclusions of the findings. Part 4 contains all references.

1 The ETHICAL project

This section describes the overall objectives of the ETHICAL project and the context in which it is set. It describes the need for action in the area of ethical handling of biomedical and biometric data and the approach adopted by the project consortium to its work.

1.1 Introduction

The ETHICAL project began in March 2009 as part of the European Commission's 7th Framework Programme. It had the following objectives:

- ⇨ To formulate an international dialogue on ethical implications of data collection, use and retention in medical and biometric applications, in three specific themes: potential data misuse, development of a unique identifier and international standardisation of ethical requirements.
- ⇨ To develop a guide on government-industry collaboration prerequisites concerning the data collection, use and retention in medical and biometric applications.
- ⇨ To develop a code of conduct for 7th Framework Programme researchers, concerning the data collection, use and retention in medical and biometric applications.
- ⇨ To identify a set of ethical requirements for international biometric and medical data sharing.

The ETHICAL project comprised a Consortium of eight organisations drawn from across the globe. These are listed in Annex A.

1.2 Mission of the ETHICAL Project

The following paragraphs set out the origins of the ETHICAL project, describing its roots in the ever-evolving and increasingly complex world of data collection and usage and supporting technologies.

1.2.1 The Ethical Context

The rapid developments in information and communication technologies, while creating new business opportunities and services, pose new threats and risks for privacy. At the same time, issues related to the protection of privacy are in all modern societies subject to both legislation and to ethical principles. Accordingly, the ETHICAL project had within its scope the following assumptions:

- ⇨ Ethics addresses principles of right and wrong. Some of these principles are used as a basis for laws.
- ⇨ Laws are tools to implement ethical principles in a given society at a given time and to provide that society with a means to prosecute infringements. Laws are official statements that encourage the enforcement of behaviour in society. Not adhering to laws may result in prosecution by a jurisdiction's legal authorities.
- ⇨ An ethical dilemma is a choice which has to be made and one which is not covered by a law.

Thus, the ETHICAL consortium concluded that ethics will be the main guidance for:

- ⇨ Topics where legislation does not yet exist.
- ⇨ Topics where legislation is incomplete or must remain ambiguous.
- ⇨ Topics that are outside the scope of legislation.

1.2.2 The Need for the Project

An international debate on the ethics of data collection, use and retention in medical and biometric applications was considered urgent. The quality and the quantity of usage of medical data and, in particular, genetic data and biometric markers are fast evolving everywhere in Europe and worldwide.

Today's networked environments change the reference framework for privacy. While innovative information and communication services are constantly improving people's lives and contribute to growth throughout the global economy, they also create new risks. The crucial issue of protecting personal data therefore becomes more complex. Processing personal data over distributed networks poses the threat of misuse. What should be defined as minimum and optimal standards to preserve privacy, and how technology can assist in the protection of integrity and privacy of data, are critical questions.

The lack of harmonisation and standardisation of international ethical principles has the potential to lead to an abuse of data collection, use and retention by organisations and individuals that seek to exploit the lack of expression of ethical standards across and between different societies. These developments raise various problems affecting the daily life of more and more citizens and therefore answers and insights into the ethical dilemmas involved are needed.

Often achievements in emerging fields of medicine and technology will be "moving targets" for legislation. Rapid progress in these two fields may raise societal questions which need to mature – with the support of ethics – before legislation can be defined, agreed and adopted.

1.3 Approach

The objective of the ETHICAL project was to facilitate debate and discussion among the ethics and scientific communities towards an international consensus on a roadmap for the protection of personal rights through the safeguarding of the ethical use of person-identifiable biological data.

The ETHICAL consortium conducted an initial scientific review of relevant literature to launch the international debate and then chose a set of key questions for debate within expert communities. This dialogue was subsequently conducted using the Delphi process. The results of the scientific research and the international dialogue with relevance for eHealth developments and applications are summarised in the following sections. In addition, the project prepared validated guidelines on issues such as international data-sharing and government-industry collaborations.

The Delphi process consisted of two stages. In Stage 1 experts were asked to provide their considered views as fully as possible in response to the key questions. The views were provided by completing an online questionnaire. In Phase 2, statements were distilled from the experts' responses and presented to them for ranking on a 5-point Likert scale which ranged from "Strongly Agree" to "Strongly Disagree". A number of the responses to Phase1 and the rankings from Phase 2 are included in this document. In preparing the second stage, the moderators classified the statements into six groupings of ethical issues that had emerged from the conduct of the initial survey. These are set out in section 2 of this report.

In addition to the formal Delphi process, a mini Delphi exercise was conducted with a number of stakeholders in the form of a facilitated and interactive discussion. The dialogue was also informed by views expressed in other stakeholder groups.

2 Ethical Principles

The work of the ETHICAL project covered a wide range of topics and involved a large amount of research consisting of literature reviews, desk research and one-to-one interviews with nominated stakeholders. However, in the body of the research (encapsulated in the project deliverable, "Code of Conduct for FP7 Researchers on medical and biometric data privacy" [Ref 1] a concise number of common principles emerged. These six principles were:

- Trust
- Privacy
- Ownership
- Dignity
- Equity
- Proportionality.

The principles are described and ETHICAL's findings summarised in the following sections of the report together with an assessment of their implications for eHealth.

2.1 Trust

eHealth technologies are becoming more and more widespread in health systems across Europe. However, while most health professionals and other health workers are familiar with their purpose and operation, this is not yet the case for most patients. Some groups of patients will be relatively familiar with information and communications technology while others – elderly individuals, for example – may be less so. Both health and care professionals and patients will have questions regarding safety (in the case of semi-invasive technologies such as blood glucose monitoring) and the use of data and information.

A recurring theme in eHealth is the need for transparency in order to engender trust among members of the patient or user community regarding the way in which information about them is handled and used by health professionals, researchers, health organisations and institutions and commercial organisations. This requirement affects all those involved

in the design, development, implementation and management of eHealth applications. The practical implication of this concept is the need for openness regarding the use of data and honesty in terms of how data will be used. This is particularly the case if new or secondary purposes of that use are to be considered or implemented in the future.

In addition, patients and citizens need to be reassured that international transfer of sensitive information is handled appropriately, that financial considerations do not override ethical data handling and that data quality is maintained in order to provide accurate and safe treatment.

2.1.1 Openness and transparency about security risks

Openness and transparency are a particular requirement in this area for researchers. In ETHICAL's work, there was a strong view identified by the Delphi consultation (and reflected in the project's proposed EC policy guidelines) that researchers should be completely open to inform the public and other project participants about the security risks related to any research and should discuss the scope and implications of their work. This openness should also include the provision of third-party consultation for participants in the research activity to receive an independent briefing. These are seen as important ethical principles that could help significantly to engender trust.

Figure 1: Delphi Stage 2 Ranking of the statement that researchers have an ethical responsibility to ensure that the subjects of their research have fully understood the implications of taking part in the research

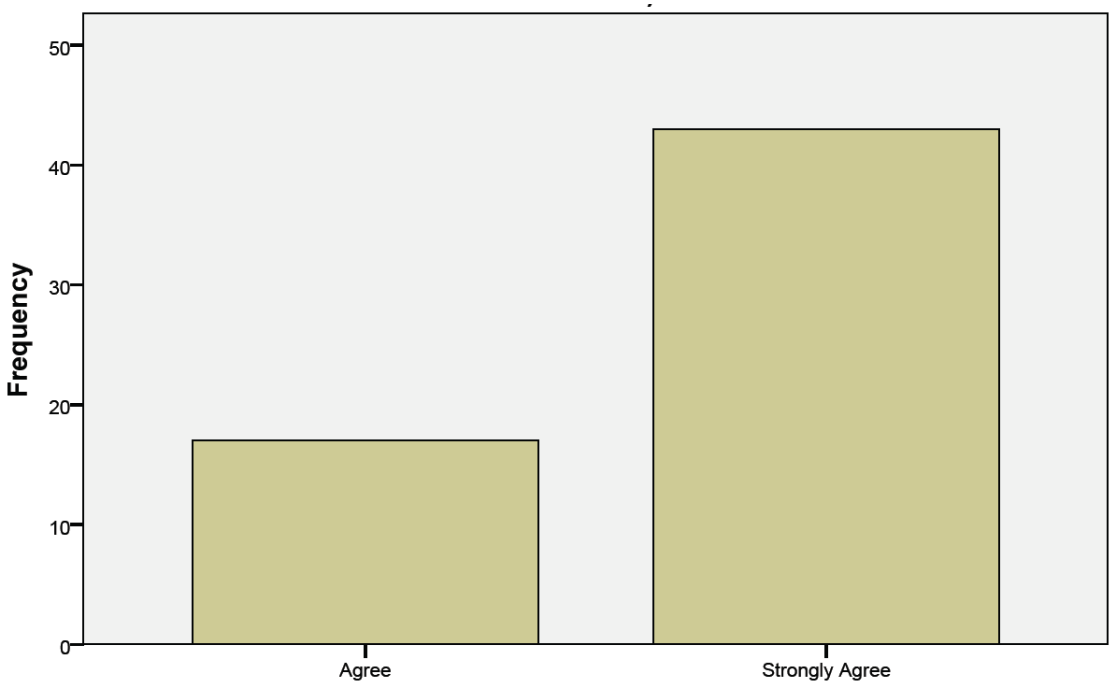
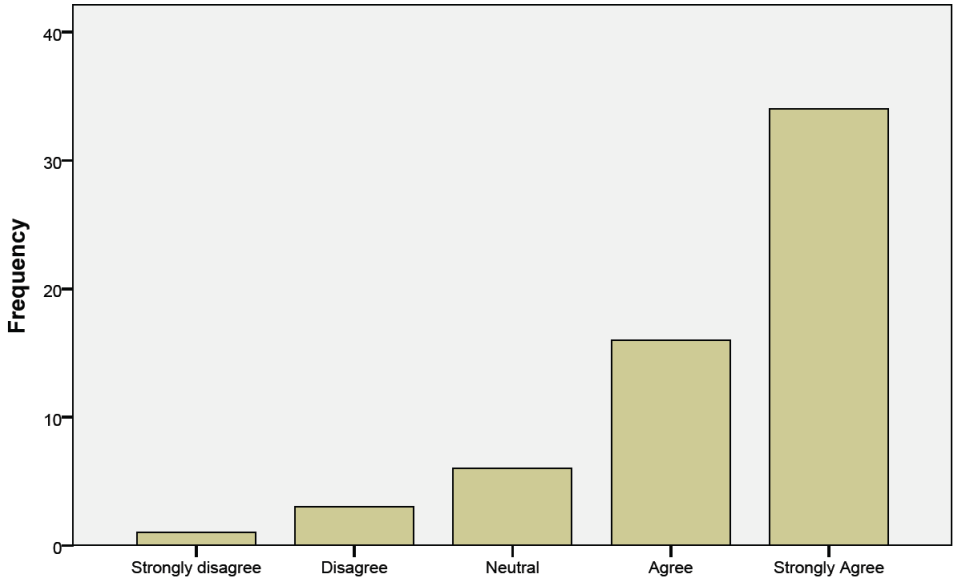


Figure 2: Delphi Stage 2 Ranking of the statement that research subjects should always have the right to receive a verbal explanation from a third party not connected with the research about how their information will be used



Issues of trust also emerge in guaranteeing the security of sensitive medical data in terms of their confidentiality, integrity and availability (i.e. when required).

One of the key Delphi exercise questions posed by ETHICAL was whether, given that security of medical data could never be guaranteed to a level of 100%, the public should learn to deal with a certain low level of risk to their privacy. The admission of such a concept might have the effect of reducing the level of trust individuals can have in those to whom they have entrusted their data. Reactions to this proposal were mixed as these extracts from the responses to Phase 1 of the Delphi exercise illustrate:

> *"Since there will be no absolute security, we have to get along with the risk of data being insecure in some ways. The question of how much risk is acceptable is at first a societal question which has to be answered by society. To come to an answer, it is important and inevitable to speak frankly about existing risks and stop the talk of no[n] realizable absolute securities. When balancing risks, it must not be forgotten that there might be individual objections which have to be taken seriously." (University Professor, Norway)*

> *"I disagree with the patronizing rhetoric of telling to the public that they 'should learn to deal with it'. Rather, one could discuss whether [there] should be a big campaign explaining [to] people that unless something dramatic is done, their rights to privacy and confidentiality are irreversibly destroyed." (Research Associate, Germany)*

In support of the notion of greater trust in data-sharing is the need for openness or transparency between data controllers and data subjects regarding breaches of data security.

Stakeholders were interviewed as part of the exercise to prepare recommendations for future EC policy directives (a formal deliverable from ETHICAL outside of the Delphi exercise). They suggested that such openness, including a requirement to inform data subjects immediately that a breach occurs, would reinforce trust. It could be argued, however, that increased frequency of security breaches might work against that suggestion.

2.1.2 The case of international transfer and sharing of medical information

Transparency also features in discussions regarding the international transfer and sharing of medical information. It has been suggested that a database of all transfers should be established. Such a database would enable individuals and organisations to determine how, where and why their data has been transferred. Indeed, manipulating individuals' data without their knowledge could be considered as dishonest and the manipulator therefore seen as untrustworthy.

The international or cross-border transfer of information raises interesting issues regarding the need for a harmonisation of rules, processes and safeguards both in Europe and globally. This would imply holding international discussions and creating international agreements. It would need a body to be involved which is recognised as being impartial and trustworthy. The World Health Organisation (WHO) was suggested as one possible body, although other bodies such as UNESCO, OECD and ISO might also be considered.

The concept of informed consent supports transparency through the need to explain to an individual exactly for what purpose he or she is being asked to give consent. Another factor affecting levels of trust about the handling of medical data arises from its use for financial gain. In considering the social and financial impacts of data handling, ETHICAL concluded that:

> *"If medical data are used as a financial source, then there is the risk that society will stop trusting healthcare practitioners and the healthcare system. One manifestation of this may be the disruption of relationships between doctors and patients. Trust and confidentiality could be breached if patients know that doctors are financially profiting from their data or allowing their data to be sold. Furthermore, some may not seek medical treatment because of the fear that their data will be sold to inappropriate parties (Smith, 2009). If patients are unaware that the data about them are sold, then they are being deceived about the nature of data flows within the medical system and society. In sum, the consequences of commoditising medical data may include a loss of trust in doctors, hospitals, and others involved in the medical system."* Ref 2

2.1.3 Risks with data quality

A final aspect of trust relates to data quality. The responsibility for data quality lies with all handlers of sensitive personal medical information who need to ensure that data is accurate. Such accuracy ensures that false conclusions cannot be drawn from the research or that individuals cannot be incorrectly identified, for example, of being at risk. This implies not only that there should be appropriate data quality mechanisms in place but also that software processing systems are properly assessed and appropriate integrity checks included.

2.1.4 Implications for eHealth deployment

The message to all stakeholders engaged in the development of eHealth initiatives is that they need to integrate resources in project planning to ensure that they have provided sufficient time for transparency in order to meet the ethical requirements of the work. This may be less of a burden for research projects (where a relatively small community of users is involved). However, this does not excuse the implementers of wider-scale initiatives from undertaking a similar exercise and, indeed, from introducing suitable governance procedures to ensure the implementation of ethical practice.

As part of its research, ETHICAL has identified a number of guidelines relating to transparency. This includes the suggestion that "health information trustees should make publicly available clear explanations of their policies, procedures, and practices regarding the collection, storage, and use of personally identifiable health information."

Associated with this statement were expectations that:

> *"The health information trustee makes publicly available, in clear and understandable language, general descriptions of its policies and practices regarding the collection, storage, and use of identifiable health care information."*
>
> *"The information [about data collection] is periodically updated and redistributed. If significant changes occur in policies or procedures, especially any changes that could result in non-consensual accessing, disclosure, or use of personally identifiable health information, relevant parties are notified of such a change."* Ref 3

2.2 Privacy

Privacy is a term that is often misunderstood and confused with confidentiality. Individuals are private people who possess knowledge about themselves and have private thoughts.

Individuals have a choice as to whether to impart information about themselves and, indeed, to choose what information to disclose. Having revealed that information, they can place a duty of confidentiality on the person to whom they have revealed it. They must trust that person to abide by that duty. In the context of healthcare, this is why the patient/professional relationship embodies a strong ethical duty of confidentiality on the part of the doctor, nurse or allied carer. This ethical duty is reinforced by international data protection legislation.

With regard to privacy, in its consideration of the ethical implications of data collection, use and retention, ETHICAL adopted the following definition:

> *"…The right of individuals to be left alone and to be protected against physical or psychological invasion or the misuse of their property. It includes freedom from intrusion or observation into one's private affairs, the right to maintain control over certain personal information, and the freedom to act without*

outside interference …" (ASTM[3], 1997 cited from Buckovich et al, 1999, p.123).
Ref 4

2.2.1 Impact of a breach of privacy

The ETHICAL project has determined that, when viewed from a society-wide level, privacy can be threatened through the collection of medical data. These threats can be manifest as a result of accidental or deliberate disclosure, the collection of data without any clear purpose or by denial of the data subject to access to his or her data. It also quotes the argument of Gavison (1980) "that violations of privacy arise when the collected information is distributed within an information network in ways the data subject has not consented to".

The impact of a breach of privacy may vary depending on the size and nature of the breach and on the sensitivity of the data held on the individual(s) concerned. For example, the single disclosure of a non-sensitive medical condition about one person may be embarrassing but not life-threatening. However, a well-publicised large-scale disclosure of such information could have societal consequences that might lead to a lowering of trust in the system and those working within it. Long-term retention of medical data means that violations of privacy can take place many years after the data was collected.

The respondents to the ETHICAL project pointed out that medical data collection in itself has implications for discrimination and stigmatisation of patients or people in general. It identified the fact that certain ethnic groups may have a tendency towards medical conditions that may be considered to be socially undesirable which may possibly lead them to be discriminated against or harmed. In addition, in some societies, certain medical conditions can bring about stigmatisation. Mental or psychological, contagious or sexually transmitted diseases may be viewed differently in various cultural or societal settings. Thus any breaches of privacy that result in such information being revealed could have very damaging consequences for individuals or groups.

2.2.2 The rights of the individual vs the rights of the community

Experts involved in the ETHICAL Delphi process commented on aspects of privacy when considering the rights of the individual as opposed to the rights of the community (public health).

The following are extracts from the experts' responses as provided in Stage 1 of the Delphi process. As these opinions were provided independently by individual experts, there is an interesting variance in the views expressed:

> *"For medical data which has a clear impact on health measures to be adopted to benefit society at large a compulsory disclosure to the state can be appropriate; however, even then there should be an obligation of the state to protect the privacy of the individual as far as is feasible."* (Research Fellow London)
>
> *"It is important to consider first the respect of individuals' privacy and confidentiality, above all in the field of health. The danger is to standardize and*

make political and economical decisions from these data. And [h]uman beings are much more complex than normalization of data. Surely, ethical standards must be debated, on the base of Natural Law and not positive law."

2.2.3 Security

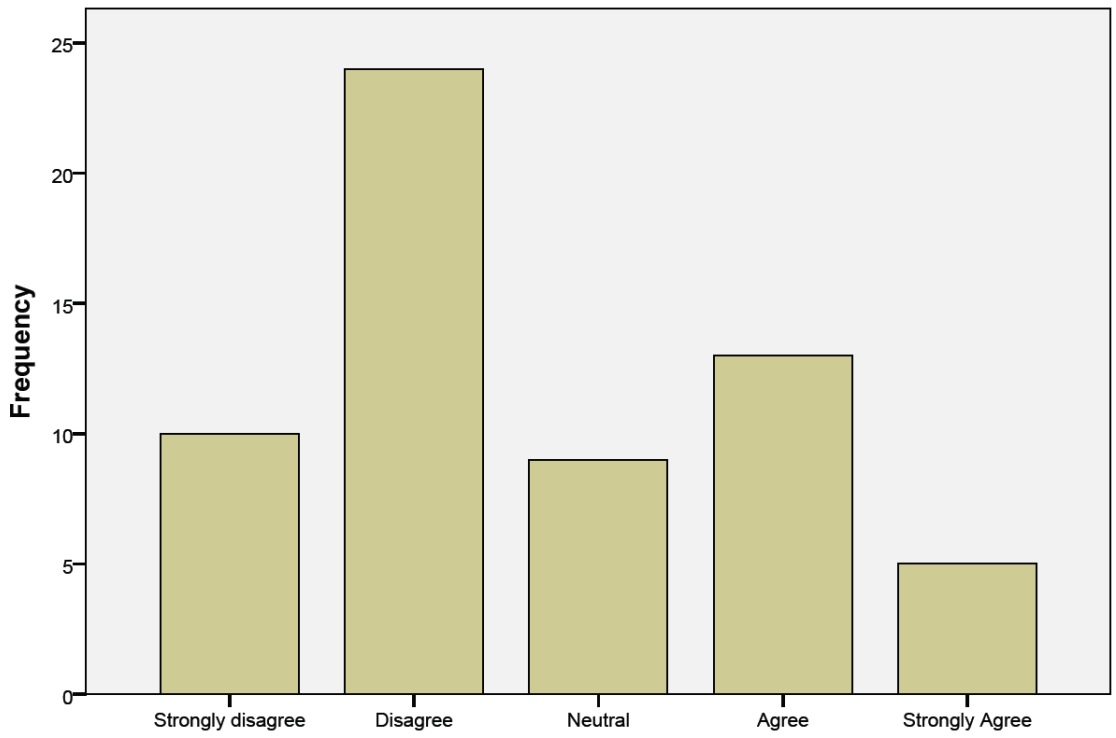
In order to protect as much as possible the privacy of personal data, organisations and individuals need to introduce appropriate security measures. In practice, this responsibility is usually that of the IT department within the medical or research institution. In the case of smaller organisations such as general or family practitioners, the responsibility for security is likely to rest with the individual doctor or, possibly, the senior partner in a practice.

Regardless of whether medical data is held in paper or electronic form it is always under threat. Such threats can come from a variety of sources. A common assumption is that information stored electronically is targeted by so-called “hackers” or can be faced with other cyber threats such as malware. While such threats are real – and there have been some notable examples in recent years – they are by no means the only ones. Simple human errors or indeed deliberate theft are also threats to sensitive data.

A key issue is what level of security to apply. This matter was raised during the Delphi exercise (see above). The general consensus seemed to be that there needs to be a formal assessment of the risks, and the likely impacts, related to personal medical data balanced against the cost of applying the security measures.

The responses to these issues are illustrated in the rankings from Phase 2 of the Delphi exercise illustrated below.

Figure 3: Delphi Stage 2 Ranking of the statement that the data subject is the only person who can define what is an acceptable level of risk to their personal medical information



2.2.4 Implications for eHealth deployment

For privacy to be addressed in an ethical manner, eHealth stakeholders will need to address the two areas of consent and security. Properly informed consent requires "disclosure of all necessary information that a reasonable person would use in making an informed decision, in a format that is readily understandable to the individual, and without coercion influencing choice." This implies that any organisation, developer, project or research unit would need to have appropriate procedures in place for this to be achieved and for these procedures to be formally documented and available. These procedures might include the ability to waive the requirement in the event that, for example, a patient's life is in danger and, due to their condition, is unable to give consent. Nevertheless, the conditions that would apply would need to be clearly documented and the whole process to be publicly accountable.

In support of processes to ensure informed consent is the requirement for all eHealth implementations to have appropriate security measures in place that are commensurate with the sensitivity of the data they hold. This implies that a formal risk analysis should be undertaken. Organisations deploying eHealth will require:

- ⇨ Written policies that define the security measures and processes that are in place to protect electronic information assets.
- ⇨ Similar policies for the protection of physical paper records.
- ⇨ Procedures and protection for the electronic transmission of sensitive data.
- ⇨ Security governance and management structures.

2.3 Ownership

2.3.1 Who owns medical data?

Data ownership is an important ethical principle that applies in many areas including medical information. The debate about who owns medical records and/or the information they contain has been discussed for many years. Opinions vary. These opinions can also vary from the legal status of personal medical data internationally:

This variation was reflected in the Delphi consultation where three categories of view were expressed. The first category supported the view that the individual providing the information i.e. the patient, is the owner of that information:

> *"Personal medical information is owned by the individual to whom it relates."*
>
> *"Individuals can never truly own their medical information because it is held by a disparate collection of organizations and institutions. They can, however, have ultimate mastery over it by defining how and when it can be used."*
>
> *"The patient has the right to have medical data deleted or amended if items can be shown to be inaccurate."*
>
> *"The withholding or suppressing of information by patients is ethical providing they are informed of the potential consequences."*

The second category of respondents were of the opinion that there is joint ownership of the information:

> *"Information is co-owned by patient and medical professional."*
>
> *"No single organization or individual can be said to own medical data. Rather each contributor to the creation of a medical record (in whatever form) can be said to have rights over certain data items."*
>
> *"The withholding or suppressing of information by patients is unethical as it place[s] [a] medical professional in potential danger of harming a patient."*

The third category took the view that:

> *"[M]edical data often represents the assessments of medical professionals which they are entitled to hold and express and the patient has no rights over these."*

In semi-structured interviews conducted with a hospital director and two medical professionals, there was a tendency to favour the joint ownership of medical records. However, this was tempered by a degree of caution regarding the care and integrity of the records. In separate discussions, patient representatives have, perhaps surprisingly, taken the view that they can never truly own their information as it is impossible for them to identify where it is held and therefore to take responsibility for it.

This concept was included as part of Phase 2 of the Delphi exercise. As the results below demonstrate, a larger number of respondents take the view that the data is owned by the person to whom it relates than by the clinician.

Figure 4: Delphi Stage 2 Ranking of the statement that individuals do not own their medical information, but they should have ultimate mastery over it by defining how and when it can be used

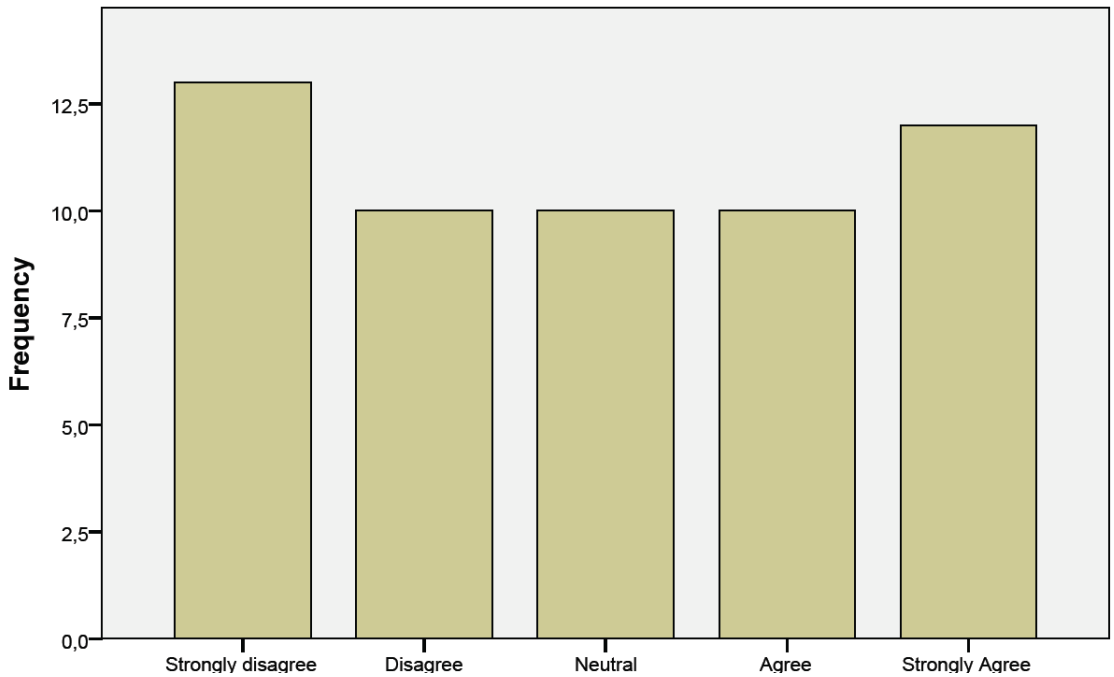


Figure 5: Delphi Stage 2 Ranking of the statement that personal medical information is co-owned by the patient and the clinician

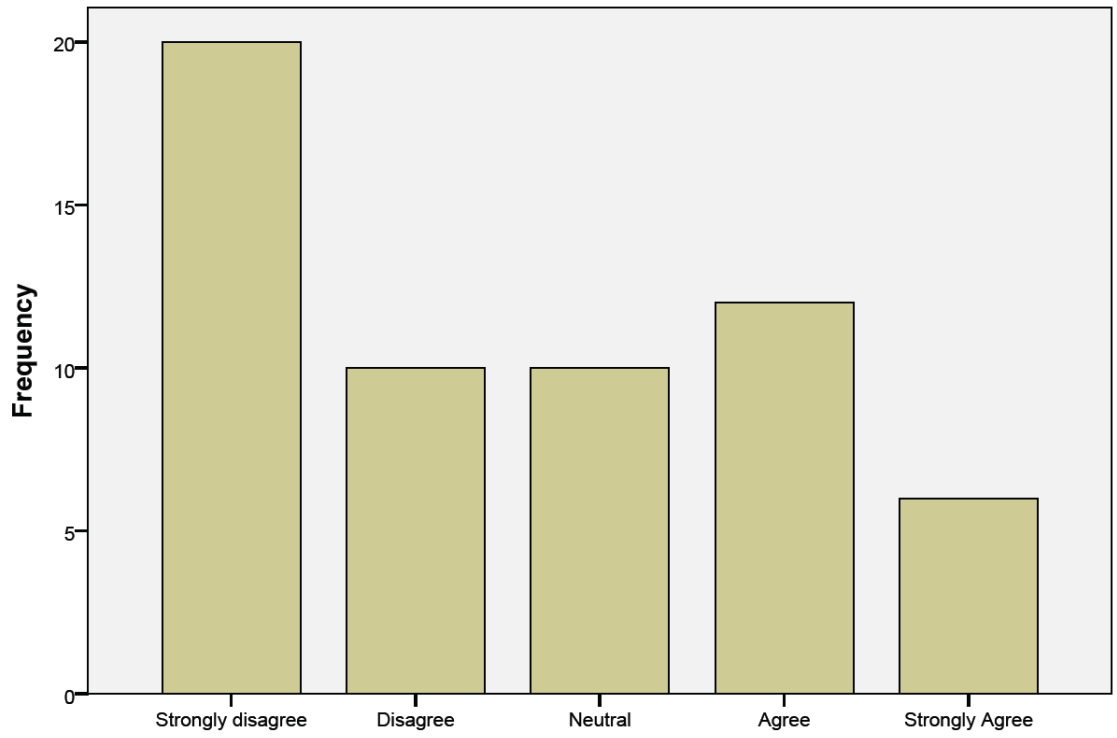
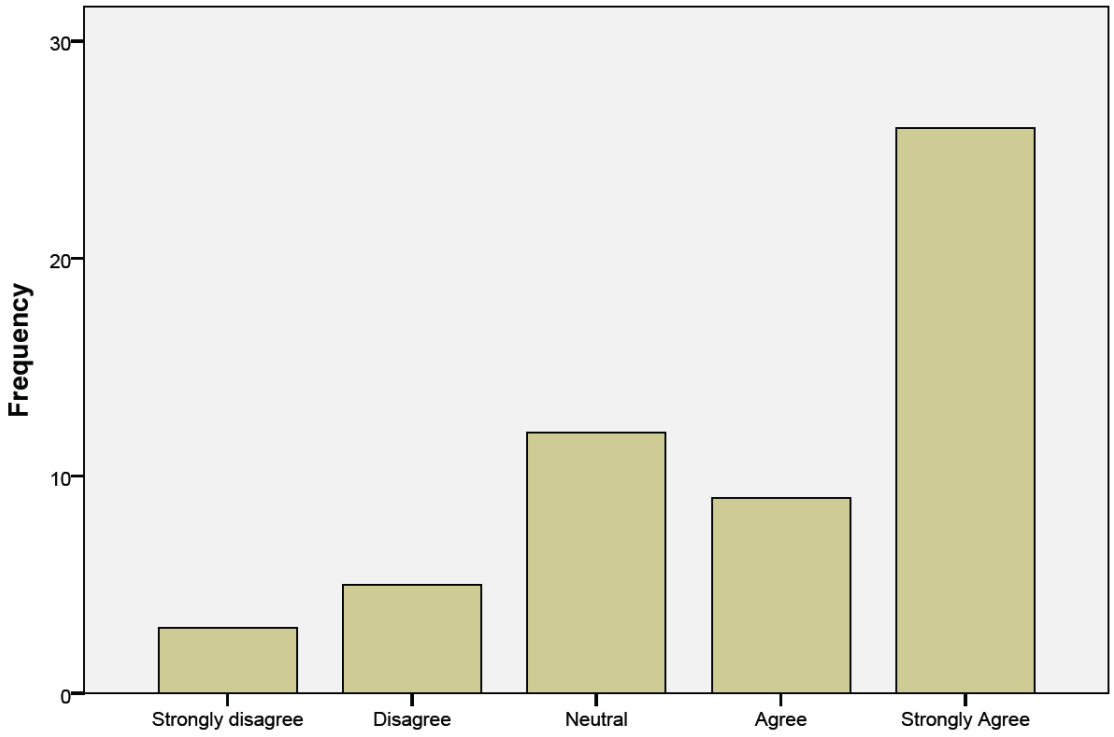


Figure 6: Delphi Stage 2 Ranking of the statement that personal medical information is owned by the individual to whom it relates



2.3.2 Ownership and data for sale

Ownership issues often come to the fore when medical data is made available for sale for profit or the recuperation of costs. Who, in these circumstances, owns the data: the seller, the purchaser, the individual to whom the data relates or the original data collector? As the ETHICAL project findings point out, in many cases neither the data subject nor the original data collector will necessarily be aware that the data has been sold. As examples, data might be sold to commercial enterprises such as insurance companies, marketing agencies, research organisations or pharmaceutical companies. However, if it is accepted that the data subject is the owner of the data as supported by the responses to the ETHICAL project Delphi survey, then sale to another party for profit without the subject's consent would be an ethical violation of that ownership.

Ownership issues are also important when considering the international transfer or sharing of personal information. Harmonisation and agreement on frameworks may address a number of the ethical issues associated with such transfers, however, they may not solve all of them particularly with reference to ownership. Allowing data controllers to transfer information legally may provide them with excessive control over data subjects' information. It would thus violate the expectations of data subjects and may be ethically wrong.

2.3.3 Implications for eHealth deployment

Unlike issues of trust and privacy where there appears to be a stronger consensus among the experts approached across the European Union, it may be that the diversity of approaches to ownership vary due to political, commercial and cultural influences in the different Member States. Although the Delphi results tend towards the view of patient or joint ownership, it may be that the concept of mastery or control is a better concept than outright possession. This is particularly appropriate in relation to the drafting of legislation and associated regulations.

However, if it is accepted – and this seems to be the case – that patients have either ownership or control of their medical records, then the question of whether they need to give consent for their data to be stored, shared or traded for any purpose has to be an integral component of the eHealth ecosystem. This implies the need for Member States to prepare position statements or legislation to address these issues. In some cases this has already happened.

In this regard, ETHICAL's findings place an emphasis on "informed" consent as distinct from reliance on the rather less defined notion of "implied" consent. It may be possible to split these two concepts according to different situations. First, implied consent to be used where the consent is clearly implied and acceptable e.g., when a patient presents for treatment to a recognised team of professionals working closely together. Second, informed consent to be used when information is needed in a wider, less defined, environment.

2.4 Dignity

2.4.1 Dignity of the person

The ETHICAL project discusses dignity from a number of perspectives. The following extracts from its report into the social and financial implications of managing medical and biometric data bring forward some of the issues relating to the way digitisation can affect the dignity of the individual

"According to Kant's (1785, reprinted 2005) famous dictum, humanity should be acted upon as ends rather than only as means. If the data controller fails to recognize the "humanity" inherent in the biometric data, and uses them only to fulfill some purpose, then he or she is violating the categorical imperative. Similarly, the European Group on Ethics in Science and New Technologies to the European Commission (1999) have put forth an opinion stating that "[p]ersonal health data form part of the personality of the individual, and must not be treated as mere objects of commercial transaction" (p. 9).

This is, essentially, a rephrasing of the categorical imperative: as medical data are constitutive of an individual's identity, they should be treated with dignity, rather than as currency that can be bought and sold."

"Specifically,information about the body can come to be considered a part of one's body. Irma van der Ploeg (2007) calls this "the informatisation of the body," or a relatively new phenomenon in which the human body appears to be redefined as an entity made of information".

Writing about genetic data in particular, van der Ploeg (2007) points out that bodies are increasingly "defined in terms of 'information' which can be processed as "digital data". In other words, one may start to see the body as made up of information such as genetic makeup, medical histories, and biometrics……It seems that loss of bodily integrity and unwanted social categorization are risks of "informatisation" (van der Ploeg, 2007). Another risk is that data controllers will be more likely to mistreat individuals if they are not physically present. Furthermore, more thought needs to be given to whether turning the body into information reduces the dignity of individuals, their identities, and their bodies."
Ref 5

2.4.2 Dignity at home

Issues of dignity also arise in relation to eHealth applications concerned with remote monitoring involving audio and video technologies. There are benefits to elderly and infirm patients of having someone monitor their wellbeing. However, it must be understood that there are times and places when the individual will not wish to be monitored. This implies the need for respect in terms of the installation of remote monitoring technologies and their operation. Such operational issues either might or should include placing the control of the monitoring technology with the individual and (if appropriate) providing the functionality to switch it off.

2.4.3 Implications for eHealth

There can be no doubt that eHealth has the potential to bring significant benefits to all stakeholders within the eHealth community. However, there is a risk that the enthusiasm to deploy the technology can ignore human sensitivities and put cost, efficiency and, to some degree, experimentation ahead of them. These factors are often at the front of the thinking of the stakeholders who deploy the technology. They are often the ones that wield more power in terms of policy and business gain in contrast to the end-user – the patient – who often does not have the power to influence such developments.

The implication is that, unless positive actions are taken, the patient relinquishes the position of being a unique human being and, instead, becomes a simple component in an eHealth machine. In order to stop this happening, eHealth developments need to be the subject of review with input from some form of patient advocacy. For such advocacy to be truly effective it needs to have recognised authority, the power of veto and, above all, needs experience and understanding of both the technology and the ethical issues associated with its deployment.

In practical terms, this means that policy makers and politicians need to reinforce their claims that "the patient is at the centre of the healthcare process" by establishing an appropriate advocacy process.

2.5 Equity

2.5.1 Solidarity equity or the individual right to equity

At a meeting in 1986, the WHO stated, "Equity in health implies that ideally everyone should have a fair opportunity to attain their full health potential and, more pragmatically, that no one should be disadvantaged from achieving this potential, if it can be avoided" Ref 6 Through its flexible and innovative nature, eHealth has the potential to support and promote equity in healthcare. It can do this through:

- ⇨ Improved access.
- ⇨ Health promotion and awareness.
- ⇨ Remote monitoring.
- ⇨ Health needs assessment.

eHealth has a number of key features that can be exploited to deliver more equitable delivery of healthcare. For instance, telemedicine enables remote communities to benefit from access to expert medical services in a way that was not possible previously as a result of geographical and transportation difficulties. The provision of tools for self-management means that people with chronic diseases can have more control over their conditions. They are no longer excluded from society by the fact that they are unable to consult with a medical professional as often as desired. Remote monitoring can also improve the quality of life for certain groups in society enabling them to spend longer in their own homes rather than being treated or cared for in nursing homes or other care centres. All of these features can work towards reducing health inequities.

However, as the findings of the ETHICAL project point out: "Equity is challenged by both the social and financial impacts of biometric and medical applications, including

surveillance systems. Social inequities can arise from stigmatisation, discrimination, exclusion, social sorting, social disadvantage, and unequal return of benefits, all of which are social impacts of the applications that have been discussed here. Financial inequities can arise when one party profits from another's personal data or when economic disparities are reinforced. One dilemma is whether "solidarity" equity, focusing on societal equity, or "individual right[s]" equity, focusing on an equal distribution across individuals, should be pursued (Gabr, p. 4).

Another is whether data users are responsible for the inequities produced by data applications. A dilemma is whether any inequities should be produced or perpetuated by data applications. Ref 7

eHealth systems in the wider sense also have the capacity to collect and monitor a large amount of medical data. The project points out that some people have argued that "there is a responsibility on the part of researchers to collect health data, family data, economic data, and other information in order to reduce disparities in the distribution of and access to health services. It might be considered a moral imperative to link demographic and medical data in order to create a more equitable society." (Rosén, 1999)

2.5.2 Implications for eHealth

While eHealth applications have the potential to promote equality and reduce inequalities in healthcare, these benefits are tempered by a number of factors. Recent discussions surrounding healthy ageing reveal a significant body of opinion that, as things currently stand, eHealth is likely to benefit the more well-off members of society. This view might be due to the fact that, at the moment, eHealth deployments are not widespread, they tend to feel experimental and their economic benefits are still the subject of evaluation.

Thus, before eHealth can be shown to be contributing to equality in healthcare, significant planning and action on the part of policy makers and a commitment to widespread investment and deployment will be required. Action to carry forward and communicate the findings of formal investigations into the benefits of eHealth can contribute to this process (if they are shown to be positive). An example of such an investigation is the scheme of three Whole System Demonstrators that has been underway in the UK with results expected during 2011. Similarly, the various eHealth large-scale pilot initiatives taking place as a result of the Competitiveness and Innovation Programme and Information and Communication Technology Policy Support Programme are encouraged to assess and evaluate their progress and outcomes.

2.6 Proportionality

2.6.1 Proportionality to balance the rights of the individual over those of society

When considering eHealth developments or, more importantly, implementing them, it is necessary to bear in mind the principle of proportionality. There are several definitions of this principle many of which are rooted in law or military action. An online reference to the Collins English Dictionary gives the definition as, "the idea that an action should not be more severe than is necessary, especially in a war or when punishing someone for a crime" Ref 8 More formally, the European Union has a principle of proportionality laid down

in Article 5 of the Treaty on European Union that regulates the exercise of powers by the European Union. It seeks to set actions taken by the institutions of the Union within specified bounds. Under this rule, the involvement of the institutions must be limited to what is necessary to achieve the objectives of the Treaties. In other words, the content and form of the action must be in keeping with the aim pursued.

As part of its work, the ETHICAL project identified a number of requirements for international data-sharing that were subsequently validated with regard to existing research and established policies. A number of these requirements were subsequently tested against the principles of proportionality including that:

- ⇨ Ethical guidelines should be sensitive and flexible depending on the purpose of the use of the data;
  - Data should not be retained longer than necessary in the recipient country;
  - Data-sharing should be unobstructed when there is an urgent need to obtain data, particularly to prevent loss of life.
- ⇨ Data should not be shared across borders via an unsecured network except in life-threatening emergencies. (See also “security”).

It was concluded that “the principle of proportionality, as reflected in the validated requirements put forth ..., can be applied in such as way as to support both the free movement of data as well as restrictions on this movement.“ Ref 9

Within an eHealth environment, and with specific reference to data collection, use and retention, the principle of proportionality can be applied in a number of areas including:

- ⇨ Public health surveillance.
- ⇨ Collection of DNA material and associated record keeping.
- ⇨ Data and system security.

In terms of public health there has been considerable debate about whether the rights of the individual are greater than those of society. In terms of proportionality, the issues pertain to whether it is acceptable to hold large amounts of information about individuals in order to deal with issues such as disease control or pandemic management. Opinions vary as to whether the rights of the individual have priority over those of society in general, as these extracts from Phase 1 of the Delphi exercise illustrate:

> *“This is a difficult political question. Different political systems have different ways of doing it. I would say that in our liberal societies we tend to give priority to individual rights over the community's interests. However, it is true, in certain severe cases when the public is in danger, only then exceptionally, priority should be given to the public good.”* (Assistant Professor, Cyprus)
>
> *“From my perspective, public health has priority over individual´s rights. That means that in cases where a conflict arises, the public health benefit should have the highest priority. On the other hand, I don´t think that individuals receiving public medical care should be obligated to provide their data to the state.*” (Associate Professor, Chile)

"The underpinning principle of all medical research ethics post-WWII is that the rights of the individuals have priority. [I agree that outbreak of infectious disease may be exception. The analysis of that case, however, should begin with an assessment of the moral duties of the individual. We may agree that the individual has a moral duty to avoid likely and significant harm to fellow citizens in such a situation. The potential and disputed benefit of medical research, however, is insufficient reason to install such a moral duty.]"
(University Professor, Norway)

2.6.2 Proportionality and DNA

The ETHICAL project addressed the specific issue of information about an individual's DNA by posing the question "Would it be ethical to collect and analyse DNA from every newborn?" Responses to this question were mixed across all levels of the dialogue. In the main, the benefits to the individual of this procedure are recognised as are the potential dangers. The dangers are seen as the use of DNA testing to identify a predisposition to a particular disease that might be used to increase insurance payments or the construction of population-wide databases for the purposes of surveillance and criminal investigation and, possibly, eugenics. Delphi Phase 2 produced the following rankings around the DNA collection proposal:

Figure 7: Delphi Stage 2 Ranking of the statement that it is totally unethical to collect and analyse DNA from every newborn

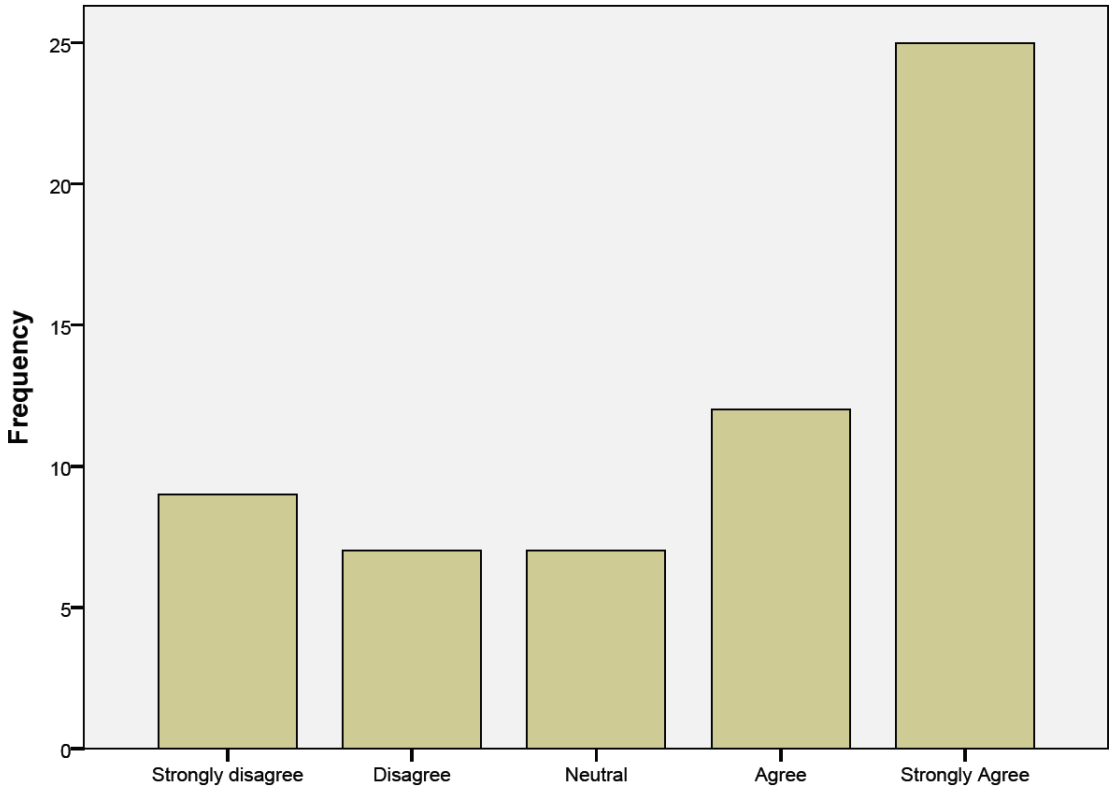
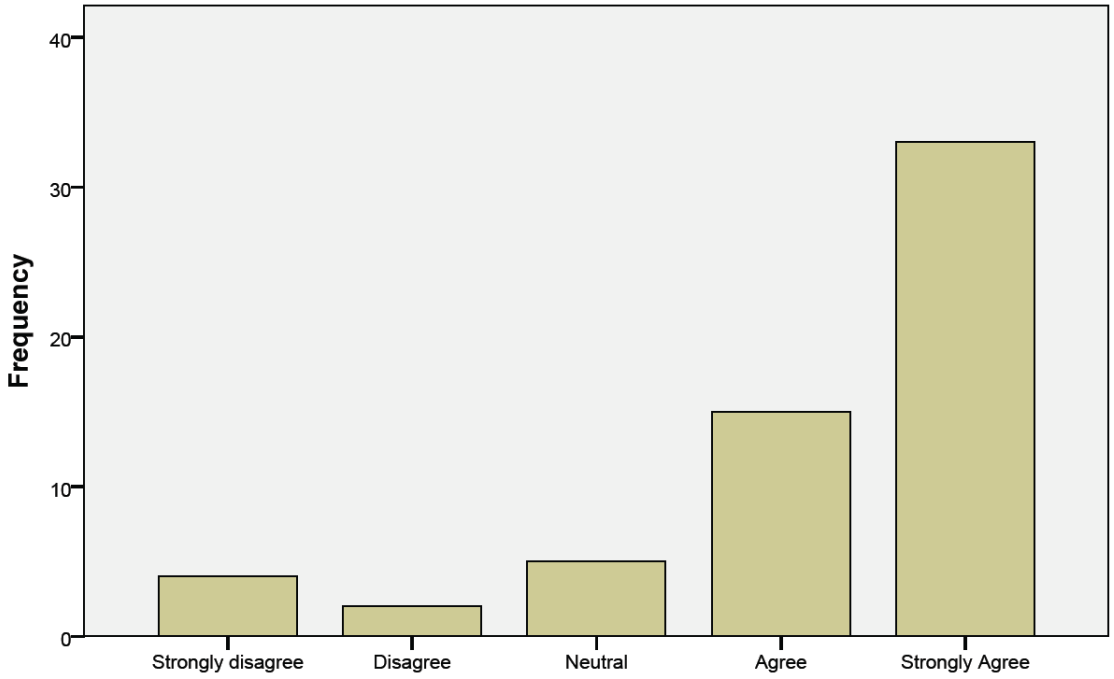


Figure 8: Delphi Stage 2 Ranking of the statement that DNA is an integral part of every individual's life and the right/permission to extract it from a newborn should be under the control of the baby's parents and not the State.



Research has revealed a number of attempts to address ethical aspects of DNA collection, all of which rely heavily on the principle of proportionality. These include the creation of universal ethical standards to cover issues such as informed consent, confidentiality, data quality, ownership, and informing individuals about the benefits of participation in research and related activities.

In terms of security, there is a clear requirement for data controllers to ensure that there are sufficient safeguards in place both in terms of technical protection and operating processes to protect the privacy of the individual. The issue is what level of security to apply to the data to be protected: it is here that issues of proportionality need to be considered. For example, the transmission of identifiable information about patients infected with HIV between medical institutions within different countries may require sophisticated and strong encryption techniques. Applying similar protection to research information regarding the incidence of influenza in particular regions may be unnecessary and disproportionate.

Achieving a proportionate response to this security question therefore requires some form of risk assessment to ensure that the degree of protection which is applied matches the assumed risk and likely impact.

2.6.3 Implications for eHealth deployment

eHealth information systems can be viewed from two different perspectives: as instruments for the delivery of effective and equitable healthcare and/or as rich sources of biomedical data that can be harvested for the purposes of medical research. In either

case, those responsible for the deployment of eHealth applications that involve the collection, use and storage of personal information will need to consider the issues of proportionality either to avoid offending ethical principles or established legislation.

This implies the use of risk and cost benefit analyses. Such analysis can balance the excessive use of security and other procedural protection that can greatly increase the cost of providing eHealth solutions and also through excessive bureaucracy introduce delay and inconvenience to the delivery process. It can also call into question the need to hold excessive amounts of information on a "just in case" basis. The temptation to use information without consent or, indeed, to store it and not use it can lead to an increase in the risk of disclosure.

The implication for eHealth deployment is that policy makers and implementers need to introduce such cost and risk analysis as part of the business case development. This might need to be included in any future guidance in this area that might be issued by the European Commission or national authorities. As with data protection legislation, a common approach to such issues with associated transparency can only lead to greater confidence in and support the wider deployment of eHealth.

3 Summary and Conclusions

There was a wide range of interest in the various stages of the ETHICAL project and the desk research and international dialogue resulted in a variety of, often differing, responses to the various ethical areas. As an indication of the nature and type of the audience involved, the project's report of the international dialogue showed the following breakdown:

> *"Out of 55 experts giving complete answers, 42 of them were from EU, 10 from other countries and 3 did not give detailed information about their country. As an approximate count their field of work was the following: 26 health care; 9 computer science; 5 law; 5 ethics; 2 sociology; 8 NA-others. They came from 19 different countries, 12 of them EU-members. The three countries with more answers (UK, Greece and Germany) account for the 44% of the answers."*

The principal conclusion that can be derived from the various items of research and dialogue is the requirement for overall guidance in the ethical handling of medical (and biometric) information. The project itself has already made suggestions, through its deliverables, for government and industry collaboration, EC policy directives and the conduct of research. These now need to be translated into formal guidance (and possibly legislation) if there is to be consistency of approach across the European Union.

4 References

The information contained in this briefing paper has drawn on a number of the ETHICAL project deliverables. They contain fuller information including more detailed references to the research material. Final versions of the documentation can be found at http://www.ethical-fp7.eu/

Ref 1: Ethical Implications of the Global Use of Digitised Biomedical and Biometric Data, Workshop Proceedings, IOS Press 2011, ISBN 978-1-60750-720-8

Ref 2: ETHICAL Project Deliverable D4.3.1, "Study on Social and Financial Impact of Data Collection, Use and Retention", p31

Ref 3: ETHICAL Project Deliverable D3.1.2, "A Study of Ethical Implications of Data Collection, Use and Retention", p69

Ref 4: ETHICAL Project Deliverable D3.1.2, "A Study of Ethical Implications of Data Collection, Use and Retention", p19

Ref 5: ETHICAL Project Deliverable D4.3.2, "Report on Social and Financial Implications of Data Collection, Use and Retention in medical and biometric applications", p22-23

Ref 6: Social justice and equity in health: report on a WHO meeting (Leeds, United Kingdom,1985). Copenhagen, Regional Office for Europe, 1986 (ICP/HSR 804/m02).

Ref 7: ETHICAL Project Deliverable D4.3.1, "Study on Social and Financial Impact of Data Collection, Use and Retention", p46

Ref 8: Reverso, Collins English Dictionary (2011), Definition of Proportionality [Online]. Available from: http://dictionary.reverso.net/english-cobuild/proportionality [Accessed 15 April 2011]

Ref 9: ETHICAL Project Deliverable D3.3.2, "Ethical Requirements for International Biometric and Medical Data Sharing", p30

Annex 1: List of Figures

The various figures contained in this report show the rankings applied to statements offered as part of the Delphi Stage 2 excercise. These were:

Annex 2:
ETHICAL Consortium:

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.
Institut Produktionsanlagen und Konstruktiontechnik, Germany

Imperial College, United Kingdom

European Health Telematics Association
Brussels, Belgium

GeoImaging Ltd, Cyprus

Palladin Institute of Biochemistry of the National Academy of Sciences of Ukraine

Universidad de Chile

University Malaysia Sarawak

Arachni Oloklиromenes Efarmoges Pliroforikis kai Robotikis EPE, Greece